



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,084	09/04/2003	Makoto Fujiwara	60188-648	4108
7590	04/02/2007		EXAMINER	
Jack Q. Lever, Jr. McDERMOTT, WILL & EMERY 600 Thirteenth Street, N.W. Washington, DC 20005-3096			SMITHERS, MATTHEW	
			ART UNIT	PAPER NUMBER
			2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/654,084	FUJIWARA ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 04 September 2003.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1,2,9,10 and 18-20 is/are rejected.
- 7) Claim(s) 3-8 and 11-17 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 04 September 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date See Continuation Sheet.
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application
- 6) Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statements filed September 4, 2003, January 14, 2004, March 16, 2004, October 11, 2005 and March 17, 2006 have been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 9, 10 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. 20040177215 granted to Nagamasa et al.

Regarding claim 1, Nagamasa meets the claimed limitations as follows:

"A semiconductor device comprising an encryption section which performs at least one of encryption and decryption of a program, wherein the encryption section includes an encryption arithmetic processing section capable of executing a plurality of sequences including an encryption process or decryption process of a program," see

paragraph [0042] (. . .The controller chip 120 is connected to other component elements . . . for controlling them.); paragraph [0046] (. . . The controller chip 120 has a function for selecting the chip . . . security process can be executed.); and Figure 22.

and an encryption control section for determining whether to permit execution of each of the sequences which can be executed by the encryption arithmetic processing section, and prohibiting the operation of the encryption arithmetic processing section with respect to a sequence whose execution is determined to be impermissible. " see paragraph [0043] (. . . The IC card chip 150 comprises: a CPU (microcomputer) for executing an arithmetic operating process; . . . a cryptography coprocessor 163 for executing processes regarding encryption/decryption; and a serial interface for transmitting and receiving data to/from the outside . . .); and Figure 26.

Regarding claim 2, Nagamasa meets the claimed limitations as follows:
"The semiconductor device according to claim 1, wherein the plurality of sequences include an encryption process or decryption process of a key. " see paragraph [0055] (. . . The controller chip 120 issues the IC card command for decrypting the result . . . by the user private key . . .); and Figure 23.

Regarding claim 9, Nagamasa meets the claimed limitations as follows:
"The semiconductor device according to claim 1, further comprising a controller for preventing accesses from the outside of the semiconductor device to the registers of the encryption arithmetic processing section and the encryption control section." see paragraphs [0042]-[0043]; paragraph [0046]; and Figures 22 and 26.

Regarding claim 10, Nagamasa meets the claimed limitations as follows:

"A semiconductor device comprising an external interface for inputting/outputting a program or data from/to an external memory, the external interface includes a program processing section for inputting/outputting a program, and a data processing section for inputting/outputting data, wherein the program processing section and the data processing section are structured independently from each other." see paragraphs [0042]-[0043] (. . . The IC card chip 150 comprises: a CPU (microcomputer) for executing an arithmetic operating process; . . . a cryptography coprocessor 163 for executing processes regarding encryption/decryption; and a serial interface for transmitting and receiving data to/from the outside . . .); paragraph [0046] (. . . The controller chip 120 has a function for selecting the chip . . . security process can be executed.); and Figures 22 and 26.

Regarding claim 18, Nagamasa meets the claimed limitations as follows:

"The semiconductor device according to claim 10, wherein the data processing section includes a through section for inputting/outputting data as it is, and a data-encryption/decryption cryptography engine for performing encryption or decryption of data at the time of input/output of the data." see paragraphs [0042]-[0043] (. . . The IC card chip 150 comprises: a CPU (microcomputer) for executing an arithmetic operating process; . . . a cryptography coprocessor 163 for executing processes regarding encryption/decryption; and a serial interface for transmitting and receiving data to/from the outside . . .); and Figure 22.

Claims 1, 2, 9, 10 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. 20030005321 granted to Fujioka.

Regarding claim 1, Fujioka meets the claimed limitations as follows:

"A semiconductor device comprising an encryption section which performs at least one of encryption and decryption of a program, wherein the encryption section includes

an encryption arithmetic processing section capable of executing a plurality of sequences including an encryption process or decryption process of a program,

and an encryption control section for determining whether to permit execution of each of the sequences which can be executed by the encryption arithmetic processing section, and prohibiting the operation of the encryption arithmetic processing section with respect to a sequence whose execution is determined to be impermissible." see paragraph [0046] (FIG 1 . . . a contact integrated circuit (or IC) card having a built-in security function. . . a CPU for controlling the whole of the microcomputer . . . reference numeral 5 denotes an encryption circuit for performing specific arithmetic computations associated with the encryption processing by using the key data . . .); and Figure 1.

Regarding claim 2, Fujioka meets the claimed limitations as follows:

"The semiconductor device according to claim 1, wherein the plurality of sequences include an encryption process or decryption process of a key." see paragraph [0046] (. . . reference numeral 5 denotes an encryption circuit for performing specific arithmetic computations associated with the encryption processing by using the key data . . .); and Figure 1.

Regarding claim 9, Fujioka meets the claimed limitations as follows:

"The semiconductor device according to claim 1, further comprising a controller for preventing accesses from the outside of the semiconductor device to the registers of the encryption arithmetic processing section and the encryption control section." see paragraphs [0066]-[0067]; paragraph [0046]; and Figure 8.

Regarding claim 10, Fujioka meets the claimed limitations as follows:

"A semiconductor device comprising an external interface for inputting/outputting a program or data from/to an external memory, the external interface includes a program processing section for inputting/outputting a program, and a data processing section for inputting/outputting data, wherein the program processing section and the data processing section are structured independently from each other." see paragraph [0046] (FIG 1 . . . a contact integrated circuit (or IC) card having a built-in security function. . . a CPU for controlling the whole of the microcomputer . . . reference numeral 5 denotes an encryption circuit for performing specific arithmetic computations associated with the encryption processing by using the key data . . .); and Figure 1.

Regarding claim 18, Fujioka meets the claimed limitations as follows:

"The semiconductor device according to claim 10, wherein the data processing section includes a through section for inputting/outputting data as it is, and a data-encryption/decryption cryptography engine for performing encryption or decryption of data at the time of input/output of the data." see paragraphs [0046] (FIG 1 . . . a contact integrated circuit (or IC) card having a built-in security function. . . a CPU for controlling the whole of the microcomputer . . . reference numeral 5 denotes an encryption circuit

for performing specific arithmetic computations associated with the encryption processing by using the key data . . . reference numeral 6 denotes an interface . . .) and [0051].

Claims 19 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. 20030005321 granted to Fujioka.

Regarding claim 19, Fujioka meets the claimed limitations as follows: "A content reproduction method, comprising the steps of: reading an original content stored in an irreproducible area of an external memory into an LSI device; generating a data inherent key in the LSI device using an inherent ID stored in an internal memory; encrypting the original content in the LSI device using the data inherent key; storing the encrypted content in a reproducible area of the external memory; reading the encrypted content stored in the reproducible area into the LSI device; decrypting the encrypted content in the LSI device using the data inherent key; and reproducing the decrypted content in the LSI device." see paragraphs [0080];[0085]-[0098] and Figures 5, 6 and 7.

Regarding claim 20, Fujioka meets the claimed limitations as follows: "The content reproduction method according to claim 19, wherein: the original content stored in the irreproducible area is a content encrypted with a data common key; prior to encryption with the data inherent key, the original content is decrypted using the data common key stored in the internal memory." see paragraphs [0080];[0085]-[0098] and Figures 5, 6 and 7.

Allowable Subject Matter

Claims 3-8 and 11-17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 3-7, the cited prior art fails to specifically teach the encryption control section includes a mode ID storage register for storing a mode ID; and the encryption control section determines whether to permit execution of each of the sequences based on the value of the mode ID stored in the mode ID storage register; a secure memory having an unrewritable area, the unrewritable area storing the mode ID, wherein the mode ID storage register is writable only at the time of boot-up of the semiconductor device; and at the time of boot-up of the semiconductor device, the mode ID read from the unrewritable area of the secure memory is written in the mode ID storage register; a boot ROM for storing a boot program, wherein writing of the mode ID in the mode ID storage register is performed by the boot program stored in the boot ROM; a secure memory for storing an installation mode flag, the installation mode flag indicating whether or not the semiconductor device is booted up for the first time, wherein the encryption control section determines whether to permit execution of each sequence while referring to the installation mode flag in addition to the value of the mode ID.

With respect to claim 8, the cited prior art fails to specifically teach a boot ROM for storing at least one boot program corresponding to one of the plurality of sequences, wherein the encryption arithmetic processing section executes the boot program stored in the boot ROM, thereby executing the sequence corresponding to the boot program.

With respect to claims 11-17, the cited prior art fails to specifically teach the program processing section includes a through section for inputting/outputting a program as it is, and a program-decryption cryptography engine for receiving an encrypted program from the external memory, decrypting the encrypted program into a raw (binary) program, and supplying the raw (binary) program to the inside of the semiconductor device; the through section includes an execution through section and an encryption through section, and a program input through the encryption through section is executed in the semiconductor device, and a program input through the encryption through section is supplied to and encrypted in an encryption section; an address segment storage register for storing address management information which represents the correspondence between respective areas of the external memory and addresses, wherein when the semiconductor device accesses the external memory to read a program, the address management information is referred to for determining which of the encryption through section, the execution through section and the program-decryption cryptography engine is activated.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Dickerson et al (US 20030212897) discloses a method for preventing access to secure areas of a semiconductor device.

B. Tugenberg et al (US 7,103,782) discloses a secure memory processing system.

C. Miyazaki et al (US 6,873,706) discloses a method for preventing attacks to a secure cryptographic device.

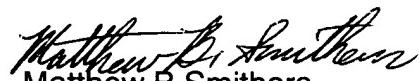
D. Kato et al (US 6,751,321) discloses a digital data reproduction device.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Matthew B. Smithers
Primary Examiner
Art Unit 2137

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date
:9/4/03;1/14/04;3/16/04;10/11/05;3/17/06.